



Powered by Accton

WA2121

IEEE 802.11b/g Mini AP Router

User Guide

User Guide

IEEE 802.11b/g Mini AP Router

IEEE 802.11b/g Wireless Router

WA2121
E062007-EK-R01
149100040200E

Table of Contents

Chapter 1: Introduction	1-1
Package Checklist	1-1
Hardware Description	1-2
LED Indicators	1-3
Ethernet RJ-45 Ports	1-3
Power Socket	1-4
Reset Button	1-4
WPS SET Button	1-4
Chapter 2: Installation	2-1
Router Mode	2-1
Bridge Mode	2-2
Chapter 3: Network Planning	3-1
Internet Gateway Router	3-1
LAN Access Point	3-2
Wireless Client	3-2
Wireless Bridge	3-3
Chapter 4: Initial Configuration	4-1
Logging into the Web Interface	4-2
Using the Setup Wizard	4-3
Chapter 5: System Configuration	5-1
System	5-3
Settings	5-3
Password	5-4
Backup and Restore	5-5
DynDNS Settings	5-6
Syslog Settings	5-7
Firmware Upgrade	5-8
WAN	5-9
WAN Settings	5-9
LAN	5-11
LAN Settings	5-11

Wireless1	5-13
Wireless-VAP1 Settings	5-13
MAC Filter Settings	5-18
Wireless2	5-19
Wireless-VAP2 Settings	5-19
WMM Settings	5-20
QoS	5-21
QoS Settings	5-21
Advanced Settings	5-22
DMZ	5-24
Status	5-25
System	5-25
Interfaces	5-26
Events Log	5-27
DHCP Clients	5-28
PPPoE	5-28
WLAN Stations	5-29
About	5-29
Reboot	5-30

Appendix A: Troubleshooting	A-1
------------------------------------	------------

Appendix B: Specifications	B-1
-----------------------------------	------------

Appendix C: License Information	C-1
--	------------

The GNU General Public License	C-1
--------------------------------	-----

Glossary

Chapter 1: Introduction

The Mini AP Router is an IEEE 802.11b/g wireless gateway router that connects your Internet access device (cable or ADSL modem) to your PC or local area network, or to its own secure wireless network.

The Mini AP Router can be automatically configured with other Wi-Fi Protected Setup (WPS) devices by simply pressing its WPS SET button. For more detailed configuration, the unit can also be set up through its easy-to-use web interface.

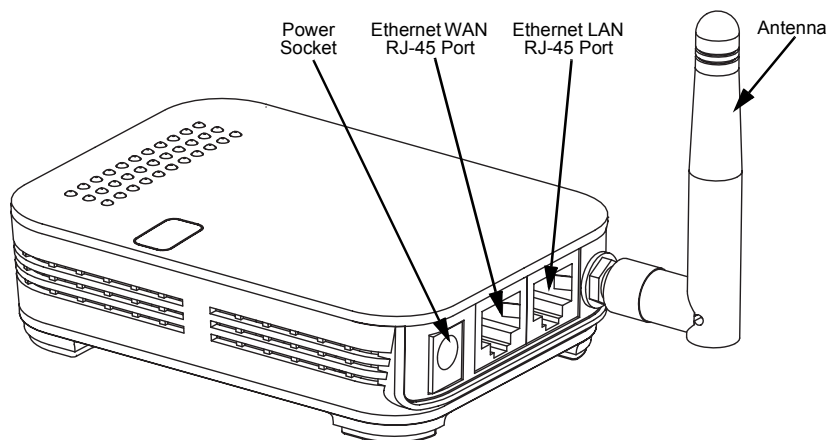
Package Checklist

The Mini AP Router package includes:

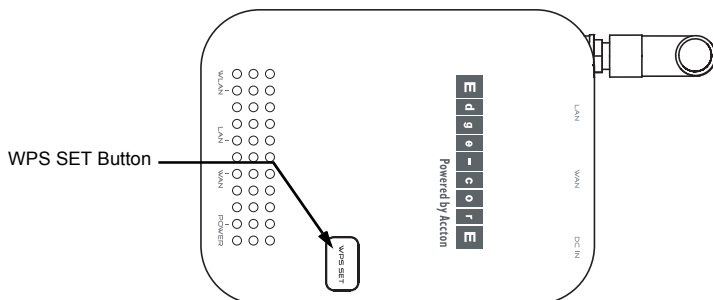
- Mini AP Router (WA2121)
- RJ-45 Category 5 network cable
- AC power adapter
- Quick Installation Guide
- User Guide CD

Inform your dealer if there are any incorrect, missing or damaged parts. If possible, retain the carton, including the original packing materials. Use them again to repack the product in case there is a need to return it.

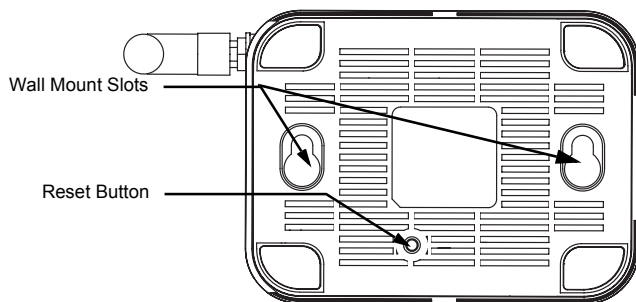
Hardware Description



Top Panel

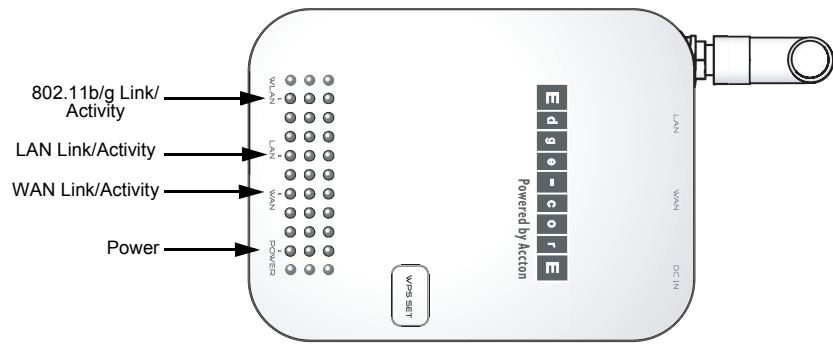


Bottom Panel



LED Indicators

The Mini AP Router includes four status LED indicators, as described in the following figure and table.



LED	Status	Description
POWER	On Green	Indicates that the system is working normally.
WAN	On/Flashing Green	Indicates a valid link on the WAN Ethernet port. Flashing indicates network activity.
	Off	The Ethernet port has no valid link.
LAN	On/Flashing Green	Indicates a valid link on the LAN Ethernet port. Flashing indicates network activity.
	Off	The Ethernet port has no valid link.
WLAN	On/Flashing Green	Indicates the 802.11b/g radio is enabled. Flashing indicates wireless network activity.
	Off	Indicates the 802.11b/g radio is disabled.

Ethernet RJ-45 Ports

The Mini AP Router has the following RJ-45 ports:

- The RJ-45 LAN port is for connection to a PC or to a 10/100 Mbps.
- The RJ-45 WAN port is for connection to a DSL or cable modem, or to a LAN or other device that provides your Internet access.

Both ports auto-negotiate the operating speed to 10/100 Mbps, the mode to half/full duplex, and the pin signals to MDI/MDI-X. Automatic MDI/MDI-X support enables you to use straight-through cables for all network connections to PCs, switches, or hubs.

Power Socket

The Mini AP Router does not have a power switch. It is powered on when connected to the AC power adapter, and the power adapter is connected to a power source. The power adapter automatically adjusts to any voltage between 100-240 volts at 50 or 60 Hz. No voltage range settings are required.

Reset Button

The Reset button can be used to restart the Mini AP Router or restore the factory default configuration. If you press the button for less than 5 seconds, the Mini AP Router will restart. If you press and hold down the button for 5 seconds or more, any configuration changes you may have made are removed and the Mini AP Router is restored to its factory default configuration.

WPS SET Button

Use the WPS SET button on the Mini AP Router to automatically connect multiple devices to the network. Within two minutes, press the physical or virtual button on wireless client devices to enable them to join the WLAN.

The WPS configuration process may be initiated on any device and there is no restriction to the order in which buttons are pressed.

Note: Any WPS-compatible devices could unintentionally join the WLAN if they are within range during the two-minute set up period after the WPS SET button is pressed.

Chapter 2: Installation

The Mini AP Router has two basic operating modes that can be set through the web management interface:

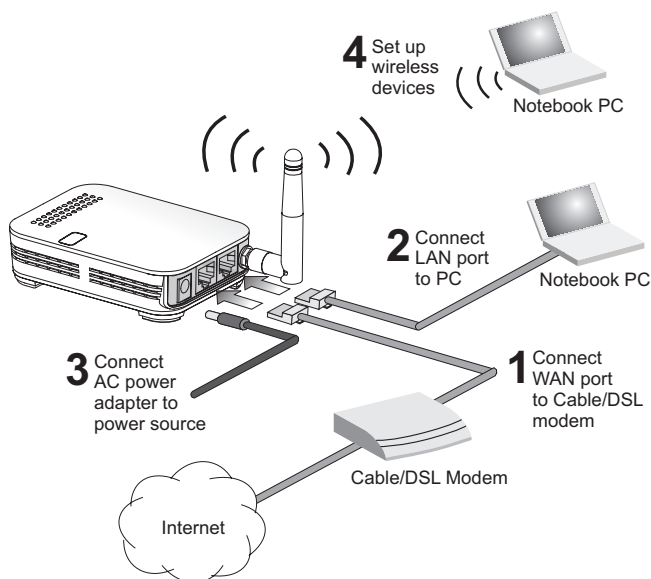
- **Router Mode** — Normal gateway mode that connects a wired LAN and wireless clients to an Internet access device, such as a cable or DSL modem. This is the factory set default mode.
- **Bridge Mode** — An access point mode that extends a wired LAN to wireless clients.

In addition to these basic operating modes, each wireless interface supports a Wireless Distribution System (WDS) link to another Mini AP Router, and a wireless client mode. These advanced configurations are not described in this section. See “Network Planning” on page 3-1 for more information.

In a basic configuration, how the Mini AP Router is connected depends on the operating mode. The following sections describe connections for basic Router Mode and Bridge Mode operation.

Router Mode

In its default Router Mode, the Mini AP Router forwards traffic between an Internet connected cable or ADSL modem, and wired or wireless PCs or notebooks. The basic connections are illustrated in the figure below.



To connect the Mini AP Router in Router Mode for use as an Internet gateway, follow these steps:

1. Connect an Ethernet cable from the Mini AP Router's WAN port to your Internet connected cable or ADSL modem.
2. Connect an Ethernet cable from the Mini AP Router's LAN port to your PC. Alternatively, you can connect to a workgroup switch to support multiple users. The Mini AP Router can support up to 253 wired or wireless users.
3. Power on the Mini AP Router by connecting the AC power adapter and plugging it into a power source.

When you power on the Mini AP Router, verify that the Power LED turns on and that the other LED indicators start functioning as described under "LED Indicators" on page 1-3.

4. Set up wireless devices by pressing the WPS Set button on the Mini AP Router or by using the web interface. See "Initial Configuration" on page 4-1 for more information on accessing the web interface.

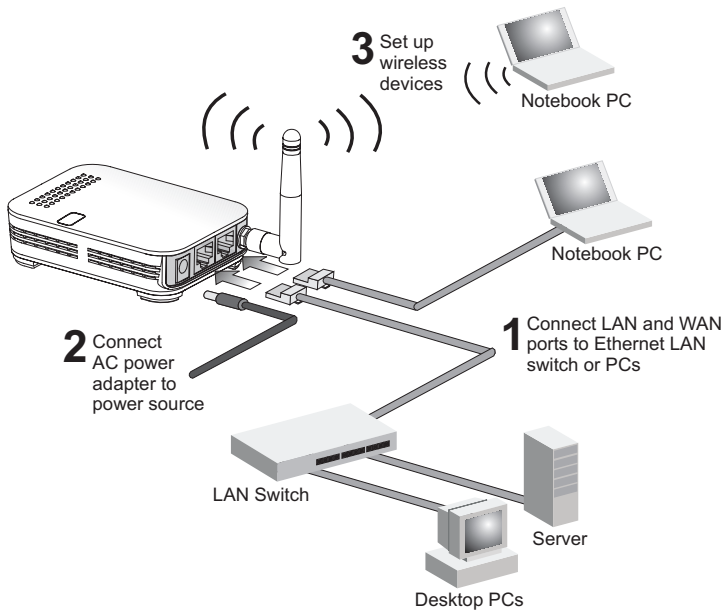
Caution: Use ONLY the power adapter supplied with the Mini AP Router. Otherwise, the product may be damaged.

Bridge Mode

In Bridge Mode, the Mini AP Router operates as a wireless access point, extending a local wired network to associated wireless clients (PCs or notebooks with wireless capability). From any nearby location, you can then make a wireless connection to the Mini AP Router and access the wired network resources, including local servers and the Internet.

In Bridge Mode, the Mini AP Router does not support gateway functions on its WAN port. Both the LAN port and the WAN ports can be connected to a local Ethernet LAN.

Note: Bridge Mode is not the factory default mode and must be manually set using the web management interface.



To connect the Mini AP Router for use as an access point, follow these steps:

1. Connect an Ethernet cable from the Mini AP Router's LAN or WAN port to your local network switch.
2. Power on the Mini AP Router by connecting the AC power adapter and plugging it into a power source.

When you power on the Mini AP Router, verify that the Power LED turns on and that the other LED indicators start functioning as described under "LED Indicators" on page 1-3.

3. Set up wireless devices by pressing the WPS Set button on the Mini AP Router or by using the web interface. See "Initial Configuration" on page 4-1 for more information on accessing the web interface.

Caution: Use ONLY the power adapter supplied with the Mini AP Router. Otherwise, the product may be damaged.

Chapter 3: Network Planning

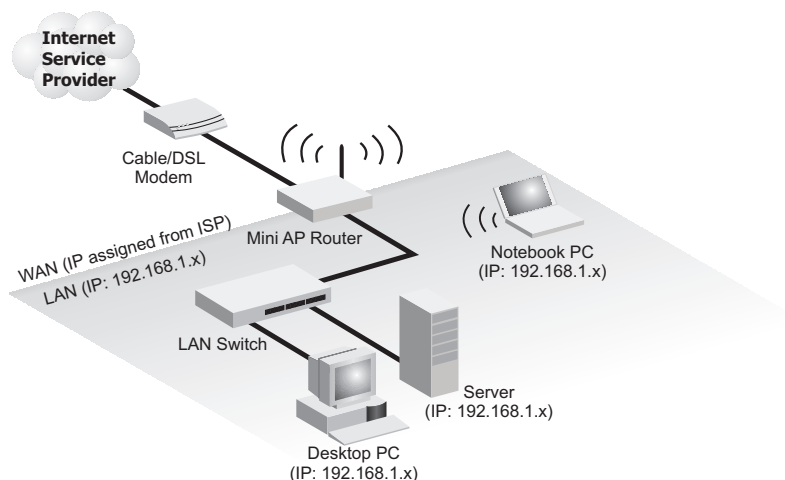
The Mini AP Router is designed to be very flexible in its deployment options. It can be used as an Internet gateway for a small network, or as an access point to extend an existing wired network to support wireless users. It also supports use as a wireless client to connect to another wireless network, or a wireless bridge to connect two wired LANs.

This chapter explains some of the basic features of the Mini AP Router and shows some network topology examples in which the device is implemented.

Internet Gateway Router

The Mini AP Router can connect directly to a cable or DSL modem to provide an Internet connection for multiple users through a single service provider account. Users connect to the Mini AP Router either through a wired connection to the LAN port, or through the device's own wireless network. The Mini AP Router functions as an Internet gateway when set to Router Mode.

An Internet gateway employs several functions that essentially creates two separate Internet Protocol (IP) subnetworks; a private internal network with wired and wireless users and a public external network that connects to the Internet. Network traffic is forwarded, or routed, between the two subnetworks.



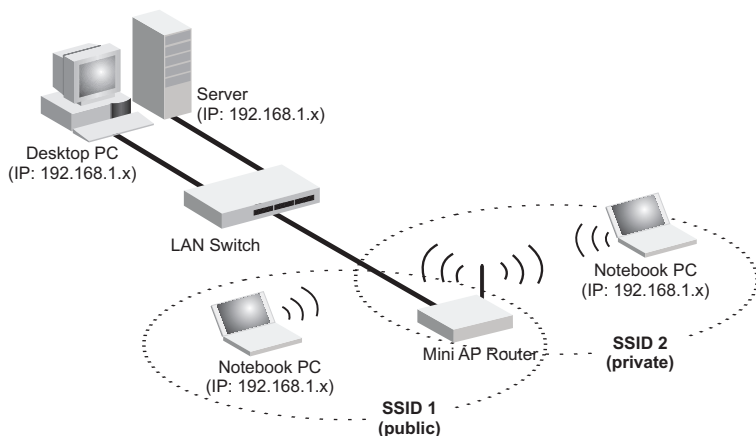
The private local network, connected to the LAN port or wireless interface, provides a Dynamic Host Configuration Protocol (DHCP) server for allocating IP addresses to local PCs and wireless clients, and Network Address Translation (NAT) for mapping the multiple "internal" IP addresses to one "external" IP address.

The public external network, connected to the WAN port, supports DHCP client and Point-to-Point Protocol over Ethernet (PPPoE) for connection to an Internet service provider (ISP) through a cable or DSL modem:

LAN Access Point

The Mini AP Router can provide an access point service for an existing wired LAN, creating a wireless extension to the local network. The Mini AP Router functions as purely an access point when set to Bridge Mode. When used in this mode, there are no gateway functions between the WAN port and the LAN and wireless interface.

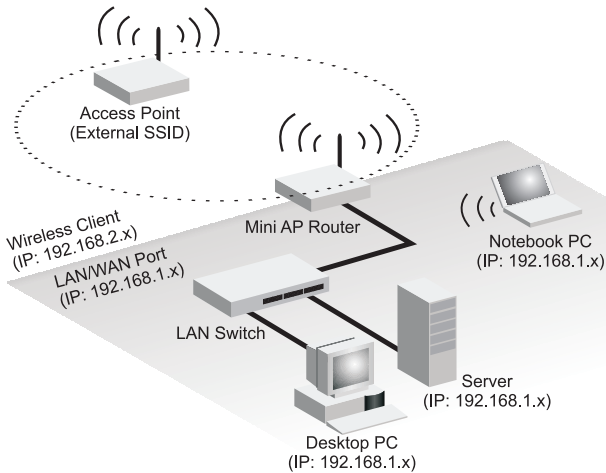
A Wi-Fi wireless network is defined by its Service Set Identifier (SSID) or network name. Wireless clients that want to connect to a network must set their SSID to the same SSID of the network service. The Mini AP Router supports two separate wireless interfaces, that is two SSIDs or Virtual Access Points (VAPs). The two VAP interfaces can be configured separately to support different security settings or other wireless functions.



Wireless Client

The Mini AP Router can operate as a wireless client on one VAP interface, which enables a connection to another wireless network.

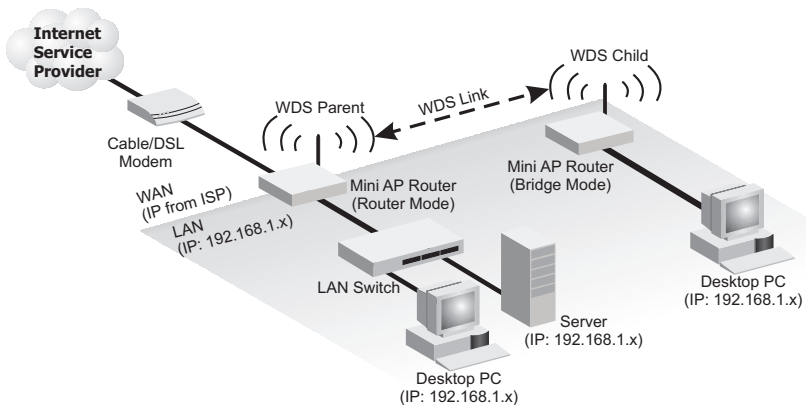
The wireless client option requires the unit to be set to Router Mode. When the wireless client option is enabled, the client VAP interface functions as the external gateway interface instead of the WAN port. The other VAP interface, LAN port, and WAN port all function as the local network within the same IP subnet.



Wireless Bridge

The IEEE 802.11 standard defines a Wireless Distribution System (WDS) for bridge connections between access points. The Mini AP Router can use WDS to forward traffic on links between units.

A single WDS bridge link can be specified for each VAP interface. One end of a link must be configured as the “WDS Parent” and the other as the “WDS Child.” A VAP interface can be configured as a WDS Parent when the Mini AP Router is set to either Router Mode or Bridge Mode, but to be configured to WDS child the unit must be set to Bridge Mode.



Chapter 4: Initial Configuration

The Mini AP Router offers a user-friendly web-based management interface for the configuration of all the unit's features. Any PC directly attached to the unit can access the management interface using a web browser, such as Internet Explorer (version 6.0 or above).

The initial configuration steps can be made through the web browser interface using the Setup Wizard. It is recommended to make the initial changes by connecting a PC directly to the Mini AP Router before installing it in its intended location. The Mini AP Router has a default IP address of 192.168.1.1 and a subnet mask of 255.255.255.0. If your PC is set to "Obtain an IP address automatically" (that is, set as a DHCP client), you can connect immediately to the web interface. Otherwise, you must set your PC IP address to be on the same subnet as the Mini AP Router (that is, the PC and Mini AP Router addresses must both start 192.168.1.x).

Logging into the Web Interface

In the web browser's address bar, type the default IP address: `http://192.168.1.1`. The web browser displays the home page.

The default Username is "root" with a default Password of "Edge-Core." Click OK to access the web management interface.

Note: It is strongly recommended that you change the default user name and password. If the default values are not changed, the management interface is not protected and anyone that can connect to the access point may be able to compromise your network security.



Figure 4-1. Login Page

Using the Setup Wizard

There are only a few basic steps you need to set up the Mini AP Router and provide a connection for network access for other wireless stations.

The Setup Wizard takes you through configuration procedures for the general network settings, such as IP configuration, wireless network name (Service Set Identifier), and wireless security. Follow these steps:

1. **Launch the Setup Wizard** – Click “Start with Setup Wizard” on the home page.

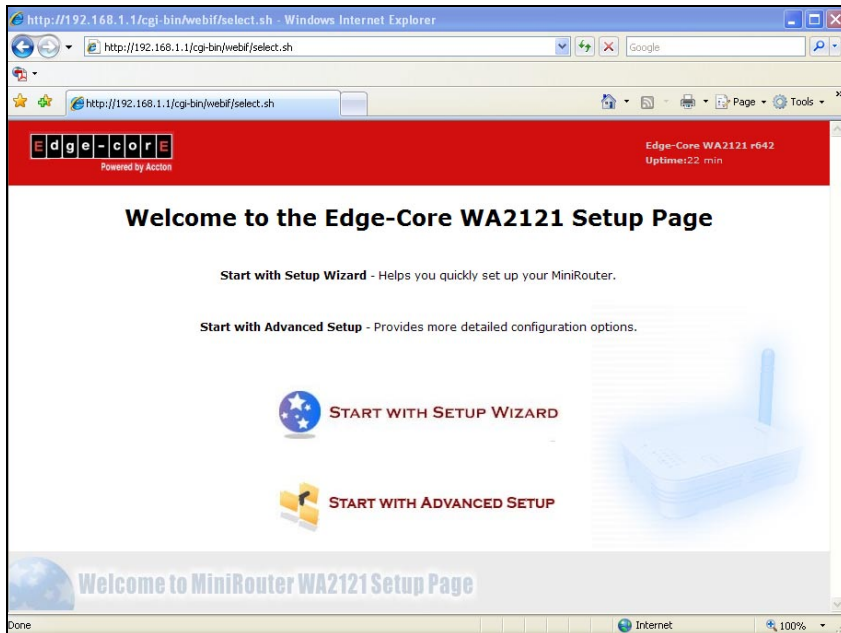


Figure 4-2. Home Page

Note: If you want to change the web interface language, select the display language from the pull-down menu.

2. **WAN Configuration** – There are three basic methods for configuring the access point's WAN port IP address.

Edge-Core WA2121 v642
Uptime: 24 min

WAN Configuration

WAN Configuration

Connection Type: ☒ DHCP ☐ Static IP ☐ PPPoE

DHCP:
Obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

Static IP:
A Static IP address is where a computer uses the same address every time a user logs on to a network, for example the Internet.

PPPoE:
PPPoE.

IP Settings

MAC Address: [][][][][][]
Clone MAC address of PC

Host Name: WA2121

MAC Address: +

Host Name: +

Back Save Next

Figure 4-3. Setup Wizard - WAN Configuration

The displayed items on this page can be described as follows:

- **DHCP** – Enables the Mini AP Router to automatically obtain an IP address from a DHCP server normally operated by the Internet Service Provider (ISP).
 - **WAN IP Address:** The IP address of the Mini AP Router. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.
 - **Subnet Mask:** The mask that identifies the host address bits used for routing to specific subnets.
 - **MAC Address:** Some ISPs limit Internet connections to a specified MAC address of one PC. This setting allows you to manually change the MAC address of the Mini AP Router's WAN interface to match the PC's MAC address provided to your ISP for registration. You can enter the registered MAC address manually by typing it in the boxes provided. Otherwise, connect only the PC with the registered MAC address to the Mini AP Router, then click the Clone MAC Address of PC button.

Notes: If you are unsure of the PC MAC address originally registered by your ISP, call your ISP and request to register a new MAC address for your account. Register the default MAC address of the Mini AP Router.
 - **Host Name:** Set the Host Name if specified by the ISP.
- **Static IP** – Select configuration for a fixed IP address xDSL Internet connection.
 - **WAN IP Address:** The IP address of the Mini AP Router. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.
 - **Subnet Mask:** The mask that identifies the host address bits used for routing to specific subnets.

- **Default Gateway** – The IP address of the gateway router that is used if the requested destination address is not on the local subnet.
 - **WAN DNS Server** – The IP address of a Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses.
 - **PPPoE** – Enable the Mini AP Router IP address to be assigned automatically from an Internet service provider (ISP) through an ADSL modem using PPPoE.
 - **Reconnect Policy**: Select a procedure for the reconnect policy.
 - **Reconnect Timeout**: The number of seconds before the next reconnect attempt. (valid range:0-600 seconds)
 - **Username**: If your ISP has provided you with a PPPoE user name, enter it in the corresponding text box.
 - **Password**: If your ISP has provided you with a PPPoE password, enter it in the corresponding text box.
 - **MTU**: Set the size of Maximum Transmission Unit (MTU) for the largest packet that the network protocol can transmit.
3. **LAN Configuration** – Configures the Mini AP Router's IP address and sets the DHCP server parameters for assigning IP addresses to wireless and LAN clients:

Edge-core
Powered by Accon

Edge-Core WA2121 r042
Uptime: 1:25

LAN Configuration

IP Settings

LAN IP Address: 192 . 168 . 1 . 1

Netmask: 255 . 255 . 255 . 0

Default Gateway: 192 . 168 . 1 . 1

LAN IP Settings:
IP Settings are optional for DHCP and PPTP. They are used as defaults in case the DHCP server is unavailable.

DHCP service For lan

DHCP service: ☐ Disabled ☒ Enabled

DHCP Start: 192.168.1.100

Max Client Q'ty: 50

DHCP Lease Time(Minutes): 60

Back Save Next

Figure 4-4. Setup Wizard - LAN Configuration

The displayed items on this page can be described as follows:

- **IP Settings** — Set the IP address configuration of the Mini AP Router.
 - **LAN IP Address** – Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. The default setting is 192.168.1.1.
 - **Netmask** – Indicate the local subnet mask is fixed as 255.255.255.0.

4 Initial Configuration

- **Default Gateway** – Normally, for wireless clients and stations in the attached LAN, the gateway address is the same as the LAN IP address. For a larger LAN with stations located on other subnets, type the IP address of the default gateway router in the text field provided.
- **DHCP Service for LAN** — Set the DHCP service configuration of the Mini AP Router.
 - **DHCP Service** – Enable the DHCP server.
 - **DHCP Start** – Specify the start IP address of a range that the DHCP server can allocate to DHCP clients. Note that the address pool range is always in the same subnet as the unit's IP setting.
 - **Max Client Q'ty** – Specify the maximum number of IP addresses to allocate to clients.
 - **DHCP Lease Time (Minutes)** – Select a time limit for the use of an IP address from the IP pool. When the time limit expires, the client has to request a new IP address.
- 4. **Wireless-VAP1 Configuration** — Sets the wireless Service Set Identifier (SSID) and wireless security encryption key for the VAP1 wireless network.

Edge-Core WA2121 r642
Uptime: 1:37

Wireless1 Configuration

Wireless Configuration

Wireless Interface: ☐ Disabled ☒ Enabled

Wlan Mode: ☒ AP+WDS Parent ☐ Client

Broadcast SSID: Yes

SSID Name: Edge-Core G1

Channel: 6

Radio Mode: ☐ 802.11b ☒ 802.11b/g

Wlan Mode:
AP+WDS Parent: AP master mode.
Client: Wireless client mode for Router.
WDS Child: WDS child mode for Bridge.

Broadcast SSID:
Broadcast ssid to every clients.

Radio Mode:
802.11b: only allow 11b clients connection.
802.11b/g: allow 11b and 11g clients connection.
Note: This is a global setting for all VAPs.

Encryption Settings

Security Mode: Disabled

Security Mode:
WPA2 allows WPA and WPA2 stations.
WPA/WPA2 with RADIUS only support for AP mode.

Back Save Next

Figure 4-5. Setup Wizard - Wireless-VAP1 Settings (AP+WDS Parent Mode)

The displayed items on this page can be described as follows:

Wireless Configuration — Enables radio communications for the VAP interface. (Default: Enabled)

- **AP+WDS Parent** – The VAP operates as an access point providing a WLAN for wireless clients. An AP using WDS can function as a wireless network bridge to allow a wireless connection between two wired network segments.

- **Broadcast SSID:** Disables SSID broadcasting to protect your network from unauthorized access. (Default: Yes)
- **SSID Name:** The name of the wireless network service provided by the VAP. Clients that want to connect to the network must set their SSID to the same as that of the VAP interface. (Default: “Wireless Network 1” for VAP1; “Wireless Network 2” for VAP2; Range: 1-32 characters)
- **Channel:** The radio channel that the Mini AP Router uses to communicate with wireless clients. When multiple access points are deployed in the same area, set the channel on neighboring access points at least five channels apart to avoid interference with each other. For example, you can deploy up to three access points in the same area using channels 1, 6, 11. Note that wireless clients automatically set the channel to the same as that used by the access point to which it is linked. (Range: 1-11)
- **Radio Mode:** Defines the radio mode for the VAP interface.
 - **802.11b:** Both 802.11b and 802.11g clients can communicate with the Mini AP Router, but 802.11g clients can only transfer data at 802.11b standard rates (up to 11 Mbps).
 - **802.11b/g:** Both 802.11b and 802.11g clients can communicate with the Mini AP Router (up to 54 Mbps).
- **Client** – Enables the Mini AP Router to operate as a client to a larger wireless network upstream from your network. In this mode the VAP operates as the WAN interface to provide Internet access. The other VAP interface, LAN and WAN ports all operate as part of the local network.
- **SSID Name:** The name of the wireless network service to which you want to connect. (Default: “Edge-Core G1” for VAP1; “Edge-Core G2” for VAP2; Range: 1-32 characters)
- **Radio Mode:** Defines the radio mode for the VAP interface.

Edge-Core
Powered by Action

Edge-Core WA2121 v642
Uptime: 2:17

Wireless1 Configuration

Wireless Configuration

Wireless Interface	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	Wlan Mode: AP+WDS Parent: AP master mode. Client: Wireless client mode for Router. WDS Child: WDS child mode for Bridge.
Wlan Mode	<input type="radio"/> AP+WDS Parent <input checked="" type="radio"/> Client	
SSID Name	<input type="text" value="Edge-Core G1"/>	
Radio Mode	<input type="radio"/> 802.11b <input checked="" type="radio"/> 802.11b/g	

Radio Mode:
 802.11b: only allow 11b clients connection.
 802.11b/g: allow 11b and 11g clients connection.
 Note: This is a global setting for all VAPs.

Figure 4-6. Wireless-VAP1 Settings (Client Mode)

Encryption Settings — Configures the encryption used by the VAP interface.

- **WEP** – Enables the Mini AP Router to use WEP shared keys. If enabled, you must configure at least one key for the VAP interface and all its clients.

Wired Equivalent Privacy (WEP) provides a basic level of security, preventing unauthorized access to the network and encrypting data transmitted between wireless clients and the Mini AP Router. WEP uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use the network.

- **Authentication Mode** – The two basic methods of authentication supported for 802.11 wireless networks are “open system” and “shared key.” Open-system authentication accepts any client attempting to connect to the access point without verifying its identity. The shared-key approach uses Wired Equivalent Privacy (WEP) to verify client identity by distributing a shared key to clients before attempting authentication.
- **Default Key** – Sets WEP key values. At least one key must be specified. Each WEP key has an index number. The selected default key is used for authentication and encryption on the VAP interface. Enter key values that match the key type and length settings. Standard keys are either 5 or 13 alphanumeric characters; or 10 or 26 hexadecimal digits.

Encryption Settings

Security Mode: WEP

Authentication Mode: ☒ Open ☐ Shared Key

Default Key: ☒ Key1 ☐ Key2 ☐ Key3 ☐ Key4

Key1:

Key2:

Key3:

Key4:

Security Mode:
WPA2 allows WPA and WPA2 stations.
WPA/WPA2 with RADIUS only support for AP mode.

WEP Key:
Standard keys are either 5 or 13 alphanumeric characters;
Or 10 or 26 hexadecimal digits.

[Back](#) [Save](#) [Next](#)

Figure 4-7. Encryption Settings - WEP Mode

- **WPA(PSK) or WPA / WPA2(PSK)** – Enable WPA(PSK) or WPA / WPA2(PSK) security on the VAP interface.

Wi-Fi Protected Access (WPA) employs a combination of technologies to provide an enhanced security solution for wireless networks. The WPA Pre-shared Key (WPA-PSK) mode for small networks uses a common password phrase that must be manually distributed to all clients that want to connect to the network. WPA / WPA2(PSK) security on the VAP interface. WPA2 is a further security enhancement that includes the now ratified IEEE 802.11i wireless security standard.

- **Pre-Shared Key:** Enter a key as an easy-to-remember form of letters and numbers. The key must be from 8 to 64 characters, which can include spaces. All wireless clients must be configured with the same key to communicate with the VAP interface.
- **Confirm Pre-Shared Key:** Enter the key for verification.

Encryption Settings

Security Mode: WPA(PSK)

Pre-shared Key:

Confirm Pre-shared Key:

Security Mode:
WPA2 allows WPA and WPA2 stations.
WPA/WPA2 with RADIUS only support for AP mode.

Pre-shared Key:
Standard keys are 8 ~ 63 alphanumeric characters or 64 hexadecimal digits.

Back Save Next

Figure 4-8. Encryption Settings - WPA(PSK) Mode

- **WPA(RADIUS) or WPA / WPA2(RADIUS)** – Enables WPA(RADIUS) or WPA / WPA2(RADIUS) security on the VAP interface.

Remote Authentication Dial-in User Service (RADIUS) is an authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of user credentials for each user that requires access to the network. A RADIUS server must be specified for the Mini AP Router to implement IEEE 802.1X network access control and Wi-Fi Protected Access (WPA) wireless security.

- **Secret Key** – A shared text string used to encrypt messages between the Mini AP Router and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string.
- **Confirm Secret Key** – Enter the key for verification.
- **RADIUS IP Address** – Specifies the IP address of the RADIUS server.
- **RADIUS Port** – The UDP port number used by the RADIUS server for authentication messages. (Range: 1024-65535; Default:1812).

Encryption Settings

Security Mode: WPA(RADIUS)

Secret Key:

Confirm Secret Key:

RADIUS IP Address:

RADIUS Port: 1812

Security Mode:
WPA2 allows WPA and WPA2 stations.
WPA/WPA2 with RADIUS only support for AP mode.

Secret Key when WPA/WPA2 (RADIUS) selected.>>

Back Save Next

Figure 4-9. Encryption Settings - WPA(RADIUS) Mode

- 5. Wireless-VAP2 Configuration** — Sets the wireless Service Set Identifier (SSID) and wireless security encryption key for the VAP2 wireless network.

Edge-Core Powered by Action

Edge-Core WA2121 r642
Uptime: 2:09

Wireless2 Configuration

Wireless Configuration

Wireless Interface: ☒ Disabled ☐ Enabled

Wlan Mode: ☒ AP+WDS Parent ☐ Client

Broadcast SSID: Yes

SSID Name: Edge-Core G2

Channel: 6

Radio Mode: ☐ 802.11b ☒ 802.11b/g

Wlan Mode:
AP+WDS Parent: AP master mode.
Client: Wireless client mode for Router.
WDS Child: WDS child mode for Bridge.

Broadcast SSID:
Broadcast ssid to every clients.

Radio Mode:
802.11b: only allow 11b clients connection.
802.11b/g: allow 11b and 11g clients connection.
Note: This is a global setting for all VAPs.

Encryption Settings

Security Mode: Disabled

Security Mode:
WPA2 allows WPA and WPA2 stations.
WPA/WPA2 with RADIUS only support for AP mode.

Back Save Next

Figure 4-10. Setup Wizard - Wireless-VAP2 Settings

Please refer to the page 4-6 to 4-9 for the details of the displayed items on this page.

Chapter 5: System Configuration

The Mini AP Router's basic settings can be configured using the Setup Wizard, as described in the previous chapter, "Initial Configuration." However, for some installations, you may need to configure specific settings that are not available in the Setup Wizard. The Advanced Setup menu provides access to all the unit's settings for complete control of the Mini AP Router's features.

To access the Advanced Setup menus, follow these steps:

1. Use your web browser to connect to the management interface using the default IP address of 192.168.1.1 or the IP address set through the Wizard.
2. Log into the Mini AP Router management interface by entering the default user name "root" and password "Edge-Core."

Note: If you want to change the web interface language, select the display language from the pull-down menu.

3. When the home page displays, click on Start with Advanced Setup.

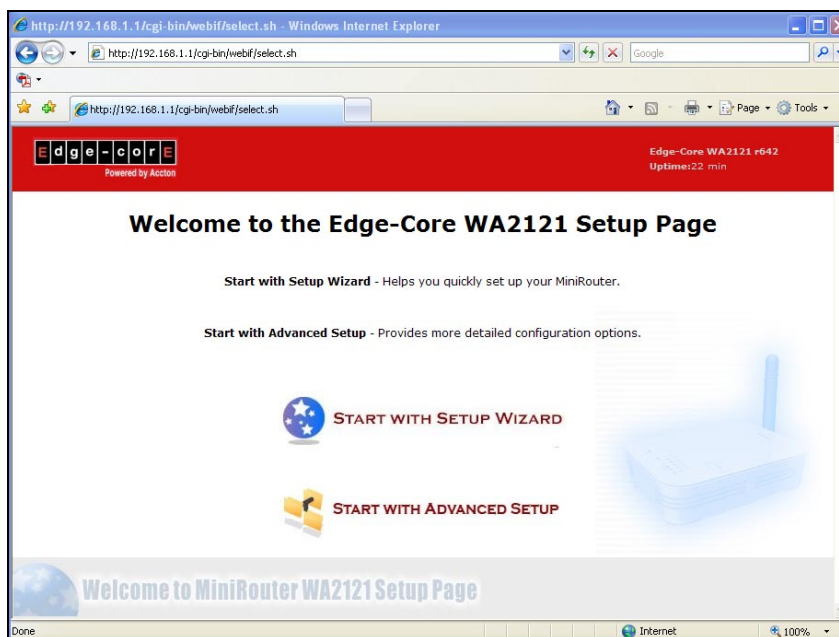


Figure 5-1. Home Page

The information in this chapter is organized to reflect the structure of the web management screens for easy reference.

The Advanced Setup pages include the options in the table below. For details on configuration for each feature, see the corresponding page number.

Table 5-1. Configuration Options		
Menu	Description	Page
<i>System</i>		5-3
Settings	Configures basic administrative settings	5-3
Password	Configures the password for management access	5-4
Backup & Restore	Backups and restores the configuration data	5-5
DynDNS	Specifies a dynamic DNS service to use	5-6
Syslog Settings	Configures the settings for syslog messages	5-6
Upgrade	Upgrades system software from a local file	5-8
<i>WAN</i>		5-9
WAN Settings	Configures IP Settings for the wide area network	5-9
<i>LAN</i>		5-11
LAN Settings	Sets the unit's IP address and configures the DHCP server for the local network	5-11
<i>Wireless1</i>		5-13
Wireless-VAP1 Settings	Enables the VAP1 interfaces and configures the settings	5-13
MAC Filter Setting	Enables the VAP1 interfaces and configures the settings	5-18
<i>Wireless2</i>		5-19
Wireless-VAP2 Settings	Enables the VAP2 interfaces and configures the settings	5-19
<i>WMM</i>		5-20
Settings	Enables Wi-Fi Multimedia (WMM) to provide basic QoS features	5-20
<i>QoS</i>		5-21
QoS Settings	Enables the QoS service and sets traffic prioritization	5-21
Advanced Settings	Edits the QoS traffic classification rules	5-22
<i>DMZ</i>		5-24
DMZ Settings	Enables the DMZ service and sets the virtual DMZ host	5-24
<i>Status</i>		5-24
System	Displays the current system status	5-25
Interfaces	Displays the current interfaces status	5-26
Events Log	Displays the system message log	5-27
DHCP Clients	Displays the DHCP client settings	5-28
PPPoE	Displays the PPPoE settings	5-28

Table 5-1. Configuration Options

Menu	Description	Page
Wireless Stations	Displays the wireless station status	5-29
About	Displays the software information	5-29
Reboot		5-30

System

The system pages allow you to manage basic system configuration settings.

Settings

The system settings page allows you to set the operation mode, time and web interface display language.

Figure 5-2. System Settings

The displayed items on this page can be described as follows:

Operation Mode – The device can be set as a router or an access point according to how you want to use the unit in your network.

- **Router** – Normal gateway mode that connects a wired LAN and wireless clients to an Internet access device, such as a cable or DSL modem. This is the factory set default mode.
- **Bridge** – An access point mode that extends a wired LAN to wireless clients.

Time Settings — Set the timezone and NTP server of the Mini AP Router.

- **Timezone** – Set your local time zone according to the location.
- **NTP Server** – Configure the IP address of an NTP time server that the Mini AP Router attempts to poll for a time update.

Password

The password page allows you to change the password for access to the management interface.

Note: Pressing the reset button on the back of the Mini AP Router for more than five seconds resets the default password “Edge-Core.”

Figure 5-3. Password

The displayed items on this page can be described as follows:

- **New Password** – The new password for management access.
- **Confirm Password** – Enter the password again for verification.

Backup and Restore

The Backup & Restore page allows you to save the Mini AP Router's current configuration or restore a previously saved configuration back to the device.

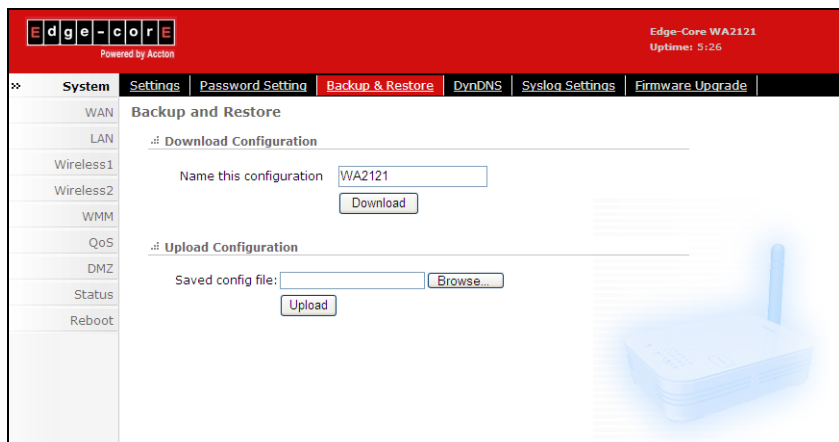


Figure 5-4. Backup and Restore

The displayed items on this page can be described as follows:

Download Configuration — Saves the current configuration to a file on the web management station. Configuration file names are given the extension ".tgz" on the management station.

- **Name this configuration** – Type a file name for the current configuration. Click Download to generate the configuration file.

Upload Configuration — Restore a previously saved configuration.

- **Save config.tgz file** – Click the Browse button to locate the saved configuration file. Then click the Submit button to restore the configuration to the Mini AP Router.

DynDNS Settings

Dynamic DNS (DDNS) provides users on the Internet with a method to tie a specific domain name to the unit's dynamically assigned IP address. DDNS allows your domain name to follow your IP address automatically by changing your DNS records when your IP address changes.

Edge-Core WA2121
Uptime: 5:54

System Settings Password Setting Backup & Restore **DynDNS** Syslog Settings Firmware Upgrade

WAN LAN Wireless1 Wireless2 WMM QoS DMZ Status Reboot

DynDNS Settings

Dynamic DNS ☒ Disabled ☐ Enabled

Service Provider zoneedit

Account

Domain Name

User Name

Password

Save Changes

Figure 5-5. DynDNS Settings

The displayed items on this page can be described as follows:

DynDNS — Enable the Dynamic DNS of the Mini AP Router.

- **Service Provider** – Specify the DDNS service provider. To set up an DDNS account, visit the websites of the service providers indicated in the table below:

Name	URL	Name	URL
ez-ip	http://www.ez-ip.net	dyns	http://www.dyns.cx
dyndns	http://www.dyndns.org	hammer node	http://www.hn.org
ods	http://www.ods.org	zoneedit	http://www.zoneedit.com
tzo	http://www.tzo.com	dyndns-static	http://www.dyndns.org
easydns	http://www.easydns.com	dyndns-custom	http://www.dyndns.org
gnudip	http://gnudip.cheapnet.net	easydns-partner	http://www.easydns.com
justlinux	http://www.justlinux.com	dhs	http://www.dhs.org

- **Domain Name** – Specify the prefix to identify your presence on the DDNS server.
- **User Name** – Specify your username for the DDNS service.
- **Password** – Specify your password for the DDNS service.

Syslog Settings

The Mini AP Router supports a logging process that controls error messages saved to memory or sent to a Syslog server. The logged messages serve as a valuable tool for isolating Mini AP Router and network problems.

Edge-Core WA2121
UpTime: 6:15

System Settings Password Setting Backup & Restore DnDNS Syslog Settings Firmware Upgrade

WAN LAN Wireless1 Wireless2 WMM QoS DMZ Status Reboot

Syslog Settings

Remote Syslog

Server IP Address

Server Port

Remote Syslog:
IP address and port of the remote logging host.
Leave this address blank for no remote logging.
The port is set to 514 by default

Local Log

Log Type

Log Size(kB)

Log Type:
Whether your log will be stored in a memory circular buffer or in a file. Beware that files are stored in a memory filesystem which will be lost if you reboot your router. Default value: circular.

Log File:
The path and name of your log file. It can be set on any writable filesystem. CAUTION: DO NOT USE A JFFS filesystem because syslog will write A LOT to it. You can use /tmp or any filesystem on an external storage unit. Default value: /var/log/messages.

Log Size:
The size of your log in Kbytes. Be careful with the size of the circular buffer as it is taken from your main memory. Default value: 16 kB.

Save Changes

Figure 5-6. Syslog Settings

The displayed items on this page can be described as follows:

Remote Syslog — Enables the logging process when a server IP address is configured.

- **Server IP Address** – The IP address of a Syslog server.
- **Server Port** – By default, the port used to listen for UDP syslog messages is 514. If you specify another port, it must be in the range of 1024 to 65535.

Local Log — Setup the file definition of the logging message.

- **Log Type** – The log type used to store the logging messages; either a memory circular buffer or in a file. Writing to a circular buffer is much faster than writing messages to a file. However, new log messages will start to overwrite old ones when the circular buffer is full. Note that all log messages are lost when the unit reboots.
- **Log File** – The path and name of your log file.
- **Log Size** – The max size of your log in Kbytes.

Firmware Upgrade

The upgrade page allows you to download a new software code file from the local web management station to the Mini AP Router using HTTP.

After upgrading to new software, the unit reboots automatically.

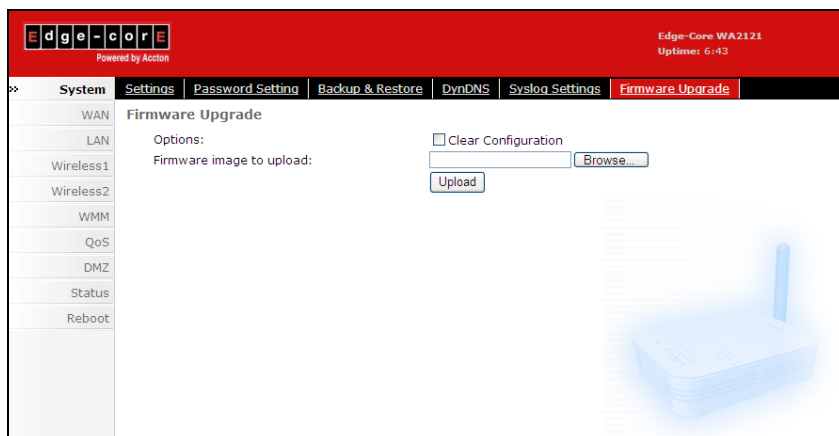


Figure 5-7. Firmware Upgrade

The displayed items on this page can be described as follows:

- **Clear Configuration** – Check the box to clear the current configuration and return to factory defaults when uploading new firmware.
- **Firmware image to upload** – Specify the name of the code file on the local web management station. You can use the Browse button to locate the image file locally on the management station. Click the Upgrade button to start the download process. Be sure to allow enough time for the download to complete before rebooting the Mini AP Router.

WAN

Specify the WAN connection parameters provided by your Internet Service Provider (ISP).

WAN Settings

Specifies the type of WAN connection to use. The selected option depends on the device connected to the WAN port and your specific ISP service.

The screenshot displays the WAN Settings interface for the Edge-Core WA2121 router. The interface is divided into a left sidebar with navigation links (System, WAN, LAN, Wireless1, Wireless2, WMM, QoS, DMZ, Status, Reboot) and a main content area. The 'WAN' tab is selected, showing the 'WAN Configuration' section. Under 'Connection Type', the 'DHCP' radio button is selected, while 'Static IP' and 'PPPoE' are unselected. To the right of these options, there are descriptive text blocks for 'DHCP', 'Static IP', and 'PPPoE'. Below the connection type section is the 'IP Settings' section, which includes a 'MAC Address' field with a 'Clone MAC address of PC' button, and a 'Host Name' field containing the text 'WA2121'. A 'Save Changes' button is located at the bottom right of the form.

Figure 5-8. WAN Settings

The displayed items on this page can be described as follows:

WAN Configuration — Set the IP address configuration of the Mini AP Router.

- **DHCP** – Enables the Mini AP Router to automatically obtain an IP address from a DHCP server.
 - **WAN IP Address:** The IP address of the Mini AP Router. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.
 - **Subnet Mask:** The mask that identifies the host address bits used for routing to specific subnets.
 - **MAC Address:** Some ISPs limit Internet connections to a specified MAC address of one PC. This setting allows you to manually change the MAC address of the Mini AP Router's WAN interface to match the PC's MAC address provided to your ISP for registration. You can enter the registered MAC address manually by typing it in the boxes provided. Otherwise, connect only the PC with the registered MAC address to the Mini AP Router, then click the Clone MAC Address of PC button.

Note: If you are unsure of the PC MAC address originally registered by your ISP, call your ISP and request to register a new MAC address for your account. Register the default MAC address of the Mini AP Router.

- **Host Name:** Set the Host Name if specified by the ISP.
- **Static IP** – Select configuration for a fixed IP address xDSL Internet connection.
 - **WAN IP Address:** The IP address of the Mini AP Router. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.
 - **Subnet Mask:** The mask that identifies the host address bits used for routing to specific subnets.
 - **Default Gateway** – The IP address of the gateway router for the Mini AP Router, which is used if the requested destination address is not on the local subnet.
 - **WAN DNS Server** – The IP address of a Domain Name Server on the service provider's network. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses.
- **PPPoE** – Enable the Mini AP Router IP address to be assigned automatically from an Internet service provider (ISP) through an ADSL modem using PPPoE.
 - **Reconnect Policy:** Select a procedure for the reconnect policy.
 - **Reconnect Timeout:** The number of seconds before the next reconnect attempt. (valid range:0-600 seconds)
 - **Username:** If your ISP has provided you with a PPPoE user name, enter it in the corresponding text box.
 - **Password:** If your ISP has provided you with a PPPoE password, enter it in the corresponding text box.
 - **MTU:** Set the size of Maximum Transmission Unit (MTU) for the largest packet that the network protocol can transmit.

LAN

The Mini AP Router must have a valid IP address for management using a web browser and to support other features. The unit has a default IP address of 192.168.1.1. You can use this IP address or assign another address that is compatible with your existing local network. The unit can also be enabled as a Dynamic Host Configuration Protocol (DHCP) server to allocate IP addresses to local PCs and wireless clients. The unit can support up to 253 local clients.

LAN Settings

The Mini AP Router includes a DHCP server that can assign temporary IP addresses to any attached host requesting the service. Addresses are assigned to clients from a common address pool configured on the unit. Configure an address pool by specifying start and end IP addresses. Be sure not to include the unit's IP address in the address pool range.

Edge-core
Powered by Accotn

Edge-Core WA2121
Uptime: 7:44

System LAN Settings

WAN LAN

Wireless1

Wireless2

WMM

QoS

DMZ

Status

Reboot

IP Settings

LAN IP Address 192.168.1.1

Netmask 255.255.255.0

Default Gateway 192.168.1.1

DHCP Service For lan

DHCP Service ☐ Disabled ☒ Enabled

DHCP Start 192.168.1.100

Max Client Q'ty 50

DHCP Lease Time (Minutes) 60

LAN IP Settings:
IP Settings are optional for DHCP and PPTP. They are used as defaults in case the DHCP server is unavailable.

DHCP Start:
The start IP address of DHCP server's IP range. The default value is 100.

Max Client Q'ty:
The maximum number of DHCP IP. The IP range is from (DHCP start) to (DHCP start + Max Client Q'ty - 1). The default value is 50.

DHCP Lease Time:
DHCP Lease Time means DHCP server grants permission to a DHCP client to use a particular IP address. The default value is 60 minutes.

Save Changes

Figure 5-9. LAN Settings

There are two operation modes:

IP Settings — Set the IP address configuration of the Mini AP Router.

- **LAN IP Address** – Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. The default setting is 192.168.1.1.
- **Netmask** – Indicate the local subnet mask is fixed as 255.255.255.0.
- **Default Gateway** – The default gateway is the IP address of the router, which is used if the requested destination address is not on the local subnet. If you have management stations located on another subnet, type the IP address of the default

gateway router in the text field provided. Otherwise, leave the address as (192.168.1.1).

DHCP Service for LAN — Set the DHCP service configuration of the Mini AP Router.

- **DHCP Service** – Enable the DHCP server.
- **DHCP Start** – Specify the start IP address of a range that the DHCP server can allocate to DHCP clients. Note that the address pool range is always in the same subnet as the unit's IP setting. The maximum clients that the unit can support is 253, but the IP pool range is determined by the start IP address and the Max Client Q'ty.
- **Max Client Q'ty** – Defines the IP pool range that the DHCP server can allocate to DHCP clients. If the start IP address is 192.168.1.1, the maximum client quantity can be up to 253. If the start IP address is 192.168.1.100, the maximum client quantity can be up to 153.
- **DHCP Lease Time (Minutes)** – Select a time limit for the use of an IP address from the IP pool. When the time limit expires, the client has to request a new IP address.

Wireless1

Set the wireless WLAN mode and wireless security for the Wireless-VAP1 network.

Wireless-VAP1 Settings

The Wireless-VAP1 Settings page includes configuration options for radio signal characteristics and wireless security features on the Mini AP Router. The Wireless-VAP1 interface is enabled by default.

Edge-core Powered by Action Edge-Core WA2121
Uptime: 7:48

System **Wireless1 Settings** MAC Filter Settings

WAN
LAN
Wireless1
Wireless2
WMM
QoS
DMZ
Status
Reboot

Wireless Configuration

Wireless Interface ☐ Disabled ☒ Enabled

Wlan Mode ☒ AP+WDS Parent ☐ Client

Broadcast SSID

SSID Name

Channel

Radio Mode ☐ 802.11b ☒ 802.11b/g

Wlan Mode:
AP+WDS Parent: AP master mode.
Client: Wireless client mode for Router.
WDS Child: WDS child mode for Bridge.

Broadcast SSID:
Broadcast ssid to every clients.

Radio Mode:
802.11b: only allow 11b clients connection.
802.11b/g: allow 11b and 11g clients connection.
Note:This is a global setting for all VAPs.

Encryption Settings

Security Mode

Pre-shared Key

Confirm Pre-shared Key

Security Mode:
WPA2 allows WPA and WPA2 stations.
WPA/WPA2 with RADIUS only support for AP mode.

Pre-shared Key:
Standard keys are 8 ~ 63 alphanumeric characters or 64 hexadecimal digits.

Wi-Fi Protected Setup

WPS Status ☒ Disabled ☐ Enabled

Wi-Fi Protected Setup:
Wi-Fi Protected Setup support a push-button connect or send a PIN (personal identification number) to network Wi-Fi devices to connect. PS. Please save changes before WPS connect.

PIN-Code:
Personal Identification Number, 8 numeric password(The build-in PIN code is 12345670).There are 2 methods to use the PIN code:
1.Enter PIN code from client application and click Send button.
2.Empty the input box and enter 12345670 in the client application and click Send button.

[Save Changes](#)

Figure 5-10. Wireless-VAP1 Settings (AP+WDS Parent Mode)

The displayed items on this page can be described as follows:

Wireless Configuration — Enables radio communications for the VAP interface. (Default: Enabled)

- **AP+WDS Parent** – The VAP operates as an access point providing a WLAN for wireless clients. An AP using WDS can function as a wireless network bridge to allow a wireless connection between two wired network segments.

- **Broadcast SSID:** Disables SSID broadcasting to protect your network from unauthorized access. (Default: Yes)
- **SSID Name:** The name of the wireless network service provided by the VAP. Clients that want to connect to the network must set their SSID to the same as that of the VAP interface. (Default: "Edge-Core G1" for VAP1; "Edge-Core G2" for VAP2; Range: 1-32 characters)
- **Channel:** The radio channel that the Mini AP Router uses to communicate with wireless clients. When multiple access points are deployed in the same area, set the channel on neighboring access points at least five channels apart to avoid interference with each other. For example, you can deploy up to three access points in the same area using channels 1, 6, 11. Note that wireless clients automatically set the channel to the same as that used by the access point to which it is linked. (Range: 1-11)
- **Radio Mode:** Defines the radio mode for the VAP interface.
 - **802.11b:** Both 802.11b and 802.11g clients can communicate with the Mini AP Router, but 802.11g clients can only transfer data at 802.11b standard rates (up to 11 Mbps).
 - **802.11b/g:** Both 802.11b and 802.11g clients can communicate with the Mini AP Router (up to 54 Mbps).
- **Client** – Select the client mode as the Mini AP Router is used to be a client to a larger wireless network upstream on your network.
 - **SSID Name:** The name of the wireless network service provided by the VAP. Clients that want to connect to the network must set their SSID to the same as that of the VAP interface.
 - **Radio Mode:** Defines the radio mode for the VAP interface.

Note: This WLAN Mode is only available when the operation mode is set to Router. Only one of the two Wireless VAPs can be set to Client mode and the other must be set to AP+WDS.

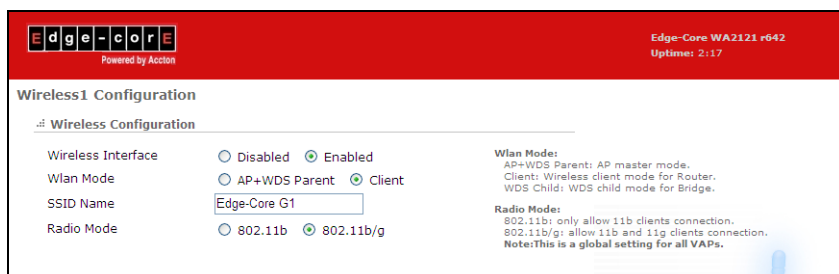


Figure 5-11. Wireless-VAP1 Settings (Client Mode)

- **WDS Child** – Select the WDS Child as the Mini AP Router is used as a bridge connect LAN and LAN between APs.
- **SSID Name:** The name of the wireless network service provided by the VAP. Clients that want to connect to the network must set their SSID to the same as that of the VAP interface.

- **Radio Mode:** Defines the radio mode for the VAP interface.

Note: This WLAN Mode is only available when the operation mode is set to Bridge. Only one of the two Wireless VAPs can be set to WDS Child mode and the other must be set to AP+WDS.

Edge-Core WA2121 v642
Uptime: 2:17

Wireless1 Configuration

Wireless Configuration

Wireless Interface ☐ Disabled ☒ Enabled

Wlan Mode ☐ AP+WDS Parent ☒ Client

SSID Name

Radio Mode ☐ 802.11b ☒ 802.11b/g

Wlan Mode:
AP+WDS Parent: AP master mode.
Client: Wireless client mode for Router.
WDS Child: WDS child mode for Bridge.

Radio Mode:
802.11b: only allow 11b clients connection.
802.11b/g: allow 11b and 11g clients connection.
Note: This is a global setting for all VAPs.

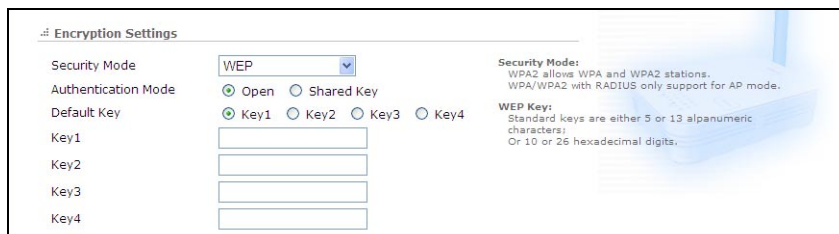
Figure 5-12. Wireless-VAP1 Settings (WDS Child Mode)

Encryption Settings — Configures the encryption used by the client.

- **WEP** – Enables the Mini AP Router to use WEP shared keys. If enabled, you must configure at least one key for the VAP interface and all its clients.

Wired Equivalent Privacy (WEP) provides a basic level of security, preventing unauthorized access to the network and encrypting data transmitted between wireless clients and the Mini AP Router. WEP uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use the network.

- **Authentication Mode:** The two basic methods of authentication supported for 802.11 wireless networks are “open system” and “shared key.” Open-system authentication accepts any client attempting to connect to the access point without verifying its identity. The shared-key approach uses Wired Equivalent Privacy (WEP) to verify client identity by distributing a shared key to clients before attempting authentication.
- **Default Key:** Sets WEP key values for one or two keys. At least one key must be specified. Each WEP key has an index number. The selected key is used for authentication and encryption on the VAP interface. Enter key values that match the key type and length settings. Standard keys are either 5 or 13 alphanumeric characters; or 10 or 26 hexadecimal digits.



Encryption Settings

Security Mode: WEP

Authentication Mode: ☒ Open ☐ Shared Key

Default Key: ☒ Key1 ☐ Key2 ☐ Key3 ☐ Key4

Key1:

Key2:

Key3:

Key4:

Security Mode: WPA2 allows WPA and WPA2 stations. WPA/WPA2 with RADIUS only support for AP mode.

WEP Key: Standard keys are either 5 or 13 alphanumeric characters; Or 10 or 25 hexadecimal digits.

Figure 5-13. Encryption Settings - WEP Mode

- **WPA(PSK)** – Enable WPA(PSK) security on the VAP interface.

Wi-Fi Protected Access (WPA) employs a combination of technologies to provide an enhanced security solution for wireless networks. The WPA Pre-shared Key (WPA-PSK) mode for small networks uses a common password phrase that must be manually distributed to all clients that want to connect to the network.

- **Pre-Shared Key:** Enter a key as an easy-to-remember form of letters and numbers. The key must be from 8 to 64 characters, which can include spaces. All wireless clients must be configured with the same key to communicate with the VAP interface. (Default: Product Serial Number)
- **Confirm Pre-Shared Key:** Enter the key for verification.



Encryption Settings

Security Mode: WPA(PSK)

Pre-shared Key:

Confirm Pre-shared Key:

Security Mode: WPA2 allows WPA and WPA2 stations. WPA/WPA2 with RADIUS only support for AP mode.

Pre-shared Key: Standard keys are 8 ~ 63 alphanumeric characters or 64 hexadecimal digits.

Figure 5-14. Encryption Settings - WPA(PSK) Mode

- **WPA / WPA2(PSK)** – Enable WPA / WPA2(PSK) security on the VAP interface.

WPA2 is a further security enhancement that includes the now ratified IEEE 802.11i wireless security standard.

- **Pre-Shared Key:** Enter a key as an easy-to-remember form of letters and numbers. The key must be from 8 to 64 characters, which can include spaces. All wireless clients must be configured with the same key to communicate with the VAP interface.
- **Confirm Pre-Shared Key:** Enter the key for verification.
- **WPS Status:** Enable Wi-Fi Protected Setup (WPS).
- **PIN-Code:** The WPS PIN (Personal Identification Number) setup is optional to the WPS button setup. It is more secure than using the WPS button. All WPS-compatible devices have their own PIN number. For each device that needs to join the network, enter its PIN number and then click Send.
- **Push Button:** Click the button to activate WPS. This action performs the same function as pressing the physical WPS SET Button on the Mini AP Router.

Note: The Wi-Fi Protected Setup is available for VAP1 only.

Encryption Settings

Security Mode: **WPA/WPA2(PSK)**

Pre-shared Key:

Confirm Pre-shared Key:

Security Mode:
WPA2 allows WPA and WPA2 stations.
WPA/WPA2 with RADIUS only support for AP mode.

Pre-shared Key:
Standard keys are 8 ~ 63 alphanumeric characters or 64 hexadecimal digits.

Wi-Fi Protected Setup

WPS Status: ☐ Disabled ☒ Enabled

Wi-Fi Protected Setup:
Wi-Fi Protected Setup support a push-button connect or send a PIN (personal identification number) to network Wi-Fi devices to connect.
PS. Please save changes before WPS connect.

PIN-Code:
Personal Identification Number, 8 numeric password(The built-in PIN code is 12345670).There are 2 methods to use the PIN code:
1.Enter PIN code from client application and click Send button.
2.Empty the input box and enter 12345670 in the client application and click Send button.

Figure 5-15. Encryption Settings - WPA/WPA2(PSK) Mode

- **WPA(RADIUS) or WPA / WPA2(RADIUS)** – Enables WPA(RADIUS) or WPA / WPA2(RADIUS) security on the VAP interface.

Remote Authentication Dial-in User Service (RADIUS) is an authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of user credentials for each user that requires access to the network. A primary RADIUS server must be specified for the Mini AP Router to implement IEEE 802.1x network access control and Wi-Fi Protected Access (WPA) wireless security. A secondary RADIUS server may also be specified as a backup should the primary server fail or become inaccessible.

- **Secret Key:** A shared text string used to encrypt messages between the Mini AP Router and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string.
- **Confirm Secret Key:** Enter the key for verification.
- **RADIUS IP Address:** Specifies the IP address or host name of the RADIUS server.
- **RADIUS Port:** The UDP port number used by the RADIUS server for authentication messages. (Range: 1024-65535; Default:1812).

Encryption Settings

Security Mode: **WPA(RADIUS)**

Secret Key:

Confirm Secret Key:

RADIUS IP Address:

RADIUS Port: **1812**

Security Mode:
WPA2 allows WPA and WPA2 stations.
WPA/WPA2 with RADIUS only support for AP mode.

Secret Key when WPA/WPA2 (RADIUS) selected.>>

Figure 5-16. Encryption Settings - WPA(RADIUS) Mode

MAC Filter Settings

Wireless clients can be authenticated for network access by checking their MAC address against a local database configured on the Mini AP Router. You can configure a list of up to 32 wireless client MAC addresses in the filter list to either allow or deny network access.

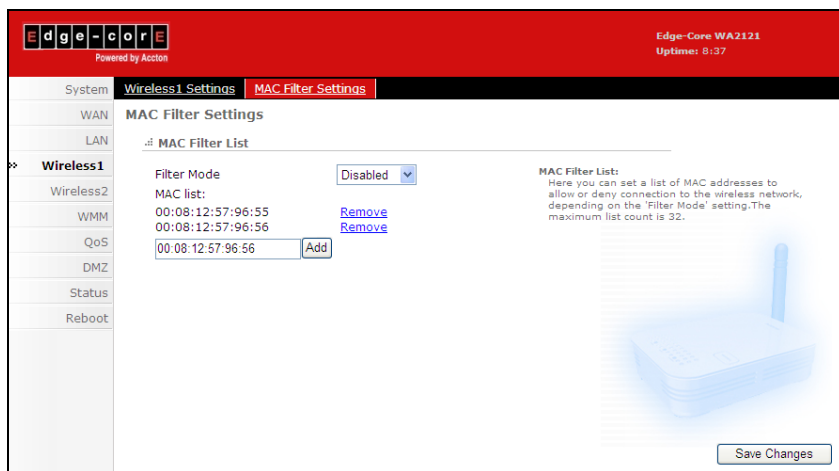


Figure 5-17. MAC Filter

The displayed items on this page can be described as follows:

- **Filter Mode** – The MAC address filter can be configured to allow or deny network access to listed clients. Select Allow to permit access or Deny to block access.
- **White List** – Specify a wireless client MAC address in the format "00:11:22:33:44:55." Click Add to add the MAC address to the filter list. To delete a MAC address from the list, click Remove next to the entry in the list.

Wireless2

Sets the wireless Service Set Identifier (SSID) and wireless security encryption key for the Wireless-VAP2 network. An SSID is a recognizable text name that identifies a wireless network. Wireless clients that want to connect to the network must set their SSIDs to match that of the router.

Wireless-VAP2 Settings

The Wireless-VAP2 Settings page includes configuration options for radio signal characteristics and wireless security features on the Mini AP Router. The Wireless-VAP2 interface is disabled by default.

The screenshot displays the 'Edge-Core WA2121' web interface. The top header is red with the 'Edge-core' logo and 'Powered by Action' text. The right side of the header shows 'Edge-Core WA2121' and 'Uptime: 8:40'. The left sidebar contains navigation links: System, WAN, LAN, Wireless1, and Wireless2 (selected). The main content area is titled 'Wireless2 Settings' and is divided into two sections: 'Wireless Configuration' and 'Encryption Settings'. In the 'Wireless Configuration' section, 'Wireless Interface' is set to 'Disabled', 'Wlan Mode' is 'AP+WDS Parent', 'Broadcast SSID' is 'Yes', 'SSID Name' is 'Edge-Core G2', 'Channel' is '6', and 'Radio Mode' is '802.11b/g'. In the 'Encryption Settings' section, 'Security Mode' is 'Disabled'. A 'Save Changes' button is located at the bottom right.

Figure 5-18. Wireless-VAP2 Settings

Please refer to the page 5-13 to 5-17 for the details of the displayed items on this page.

WMM Settings

Wi-Fi Multimedia (WMM), also known as Wireless Multimedia Extensions (WME), is a Wi-Fi Alliance interoperability certification. It provides basic Quality of Service (QoS) features for IEEE 802.11 wireless network.

The WMM settings page allows you to enable the WMM service. The specification provides prioritization of data packets based on four categories - voice, video, best effort, and background.

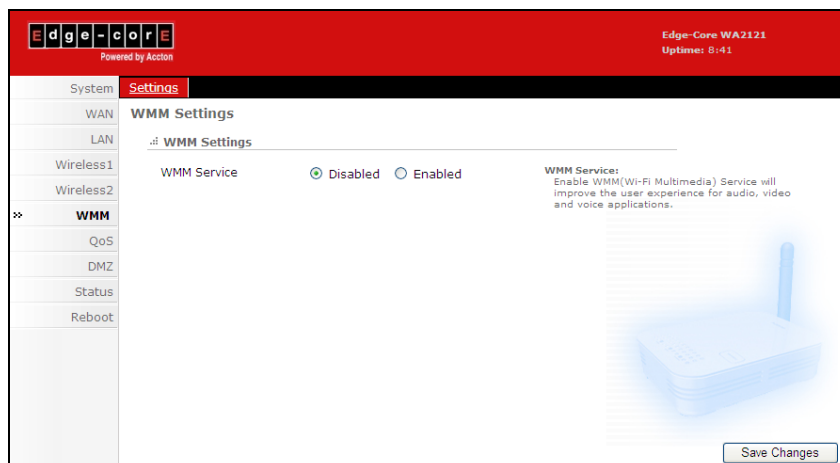


Figure 5-19. WMM Settings

The displayed items on this page can be described as follows:

- **WMM Service** – Enables the transition from data-only use of Wi-Fi into voice, audio, and video applications. (Default: Disabled)

QoS

Wireless networks offer an equal opportunity for all devices to transmit data from any type of application. Although this is acceptable for most applications, multimedia applications (with audio and video) are particularly sensitive to the delay and throughput variations that result from this equal opportunity wireless access method. For multimedia applications to run well over a wireless network, a Quality of Service (QoS) mechanism is required to prioritize traffic types and provide an “enhanced opportunity” wireless access method.

The Mini AP Router implements QoS using the Wi-Fi Multimedia (WMM) standard. Using WMM, the min router is able to prioritize traffic and optimize performance when multiple applications compete for wireless network bandwidth at the same time. WMM employs techniques that are a subset of the IEEE 802.11e QoS standard and it enables the Mini AP Router to interoperate with both WMM-enabled clients and other devices that may lack any WMM functionality.

QoS Settings

The QoS settings page allows you to enable the QoS settings and specify the WAN upload and download speeds.

Figure 5-20. QoS Settings

The displayed items on this page can be described as follows:

- **QoS Service** – Enables QoS settings of the Mini AP Router. (Default: Disabled)
- **WAN Upload Speed / Download Speed** – The maximum upload and download speeds of the Internet connection on the WAN port. It is recommended that you set these values at between 85-90% of your true speeds. Most broadband services are

rated in Megabits per second (Mbps). To convert Mbps to Kilobits per second (Kbps), multiply the value by 1024. The following table lists the most common broadband service speeds.:

Mbps	Kilobits
1	1024
2	2048
3	3072
4	4069
6	6144
8	8192
12	12288

Advanced Settings

The advanced settings page allows you to edit or create QoS Traffic Classification Rules.

The screenshot shows the Edge-Core WA2121 web interface. The top navigation bar includes 'System', 'QoS Settings', and 'Advanced Settings'. The left sidebar lists various system settings: System, WAN, LAN, Wireless1, Wireless2, WMM, QoS, DMZ, Status, and Reboot. The main content area is titled 'Advanced Settings' and contains a section for 'QoS Traffic Classification Rules'. This section displays a table with columns for Group, Src IP, Dest IP, Protocol, Layer7, Port range, and Ports. The table lists several rules, including Bulk, Priority, Normal, and Express, each with associated IP addresses, protocols, and port ranges. To the right of each rule are 'edit' and 'remove' links. Below the table is a 'new rule' link. A 'QoS Rule Edit' form is also visible, allowing users to modify a rule. This form includes fields for 'Classify As', 'Source IP', 'Dest IP', 'Protocol', 'Ports', 'Port Range', 'Layer7', and 'Peer-2-Peer'. To the right of the form, there is explanatory text about Layer-7 filters and Peer-2-Peer filters. A 'Save Changes' button is located at the bottom right of the page.

Group	Src IP	Dest IP	Protocol	Layer7	Port range	Ports	
Bulk			peer-2-peer				edit remove
Bulk			edonkey				edit remove
Bulk			bittorrent				edit remove
Priority					22,53		edit remove
Normal			tcp		20,21,25,80,110,443,993,995		edit remove
Express					5190		edit remove

[new rule](#)

QoS Rule Edit

Classify As:

Source IP:

Dest IP:

Protocol:

Ports:

Port Range:

Layer7:

Peer-2-Peer:

QoS Rule Edit:
You need only set fields you wish to match traffic on. Leave the others blank.

Layer-7:
Layer-7 filters are used to identify types of traffic based on content inspection. Numerous layer-7 filters are available on the web, though not all are efficient and accurate. To install more filters, download them and put them in /etc/l7-protocols.

Peer-2-Peer:
The difference between the Peer-2-Peer field and layer-7 filters is simply that the Peer-2-Peer option uses a special tool, ip2p, to match traffic of common p2p protocols. It is typically more efficient than layer-7 filters.

[Save Changes](#)

Figure 5-21. Advanced Settings

The displayed items on this page can be described as follows:

Qos Traffic Classification Rules – A traffic classification rule can classify traffic according to the traffic classification policy set by the network administrator, such as the combination of source addresses, destination addresses, MAC addresses, IP protocol or the port numbers of the applications.

Click edit or remove to modify the rules, or click “new rule” to create a new traffic classification rule.

Qos Rule Edit — Set the fields that you wish to match traffic on. Leave the others blank.

- **Classify As** – Select the QoS classification for the type of traffic.
 - **Bulk**: low priority, such as file transfers
 - **Normal**: Medium-throughput data only sensitive to long delays
 - **Priority**: Time sensitive traffic, such as video
 - **Express**: Time sensitive traffic, such as voice
- **Source IP** – Classify traffic based on the source IP address.
- **Dest IP** – Classify traffic based on the destination IP address.
- **Protocol** – Select TCP or UDP as the supported protocol.
- **Port** – Classify traffic by TCP/UDP port numbers. Multiple port numbers can be entered separated by commas.
- **Port Range** – Classify traffic by a TCP/UDP port number range.
- **Layer 7** – Classify traffic based on Layer 7 application protocol information.
- **Peer-2-Peer** – Classify traffic based on peer-to-peer application protocol information.

DMZ

If you have a client PC that cannot run an Internet application properly from behind the NAT firewall, you can open the client up to unrestricted two-way internet access by defining a virtual-DMZ (virtual-demilitarized-zone) host.

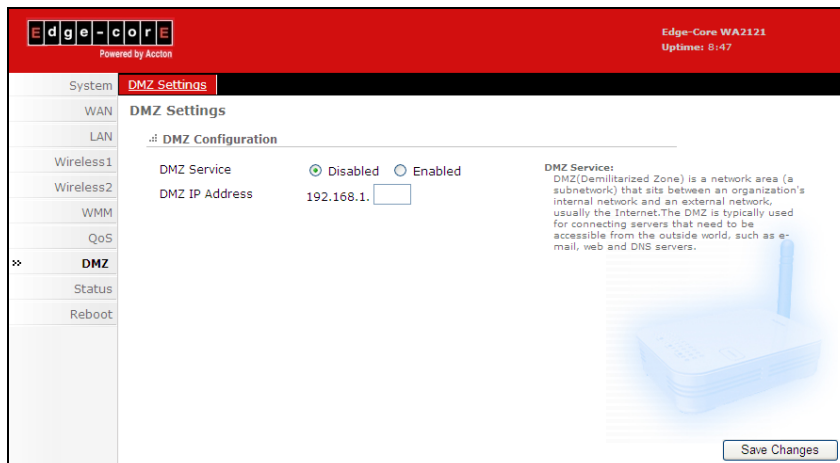


Figure 5-22. DMZ Settings

The displayed items on this page can be described as follows:

- **DMZ Service** – Enables the DMZ feature. (Default: Disabled)
- **DMZ IP Address** – Specifies the IP address of the virtual DMZ host.

Note: Adding a host to the DMZ may expose your local network to a variety of security risks, so only use this option as a last resort.

Status

The status pages display details on the current configuration and status of the Mini AP Router, including associated wireless stations and event log messages.

System

The system page displays basic system configuration settings. The displayed settings are for status information only and are not configurable on this page.

Edge-core Powered by Action Edge-Core WA2121 Uptime: 2 min

System | **System** | Interfaces | Events log | DHCP Clients | PPPoE | WLAN Stations | About

System

WAN

LAN

Wireless1

Wireless2

WMM

QoS

DMZ

» **Status**

Reboot

System

Device Edge-Core WA2121 - MR3202A-FLF-38

Board Atheros AR5315

Firmware Version v1.0 r642

WAN

IP Address

WAN Status: WAN stands for Wide Area Network and is usually the upstream connection to the internet.

LAN

IP Address 192.168.1.1

LAN Status: LAN stands for Local Area Network.

WLAN

Wireless1 Enabled

SSID Edge-Core G1

Frequency 2.437 Ghz

Encryption Off

Wireless2 Disabled

WLAN Status: WLAN stands for Wireless Local Area Network.

Figure 5-23. System

The displayed items on this page can be described as follows:

System — Displays the basic device information:

- **Device** – The device name and model number.
- **Board** – The WLAN chipset used in the Mini AP Router.
- **Version** – The version number of the current Mini AP Router software.

WAN — Displays the basic WAN status.

- **IP Address** – The IP address specified or assigned by the Internet Service Provider.
- **DNS Server 1** – Address of the ISP's DNS server.

LAN — Displays the basic LAN status.

- **IP Address** – The IP address configured on the Mini AP Router.

WLAN — Displays the basic WLAN information:

- **VAP1/VAP2** – The status of the VAP interface.
- **ESSID** – The service set identifier for this wireless group.
- **Frequency** – The The channel frequency being used by the radio.
- **Encryption** – The encryption used by the VAP interface.

Interfaces

The Interfaces page displays the settings for each wireless interface. The displayed settings are for status information only and are not configurable on this page.

The screenshot shows the web interface of an Edge-Core WA2121 router. The top navigation bar includes links for System, Interfaces (selected), Events log, DHCP Clients, PPPoE, WLAN Stations, and About. The main content area is titled 'Interfaces' and shows a summary of network interfaces. On the left, a sidebar menu lists various system settings like WAN, LAN, Wireless1, Wireless2, WMM, QoS, DMZ, Status (selected), and Reboot. The main area displays three interface sections: WAN, LAN, and WLAN. Each section shows MAC Address, IP Address, Received/Transmitted packet counts, and status information. A 'Show raw statistics' button is at the bottom.

Interface	MAC Address	IP Address	Received	Transmitted	Status
WAN	00:12:CF:3F:7E:42	192.168.1.1	0 pkts (0.0 B)	3.1K pkts (1023.3 KiB)	WAN Status: WAN stands for Wide Area Network and is usually the upstream connection to the internet.
LAN	00:12:CF:3F:7E:42	192.168.1.1	229 pkts (23.5 KiB)	2.7K pkts (1.0 MiB)	LAN Status: LAN stands for Local Area Network.
WLAN	00:12:CF:3F:7E:43	Edge-Core G1	2.437 Ghz	18 dBm	WLAN Status: WLAN stands for Wireless Local Area Network.

Figure 5-24. Interfaces

The displayed items on this page can be described as follows:

WAN – Display the basic WAN configuration settings.

- **MAC Address** – MAC address of the Mini AP Router on its WAN port.
- **IP Address** – The IP address assigned for the WAN interface.
- **DNS Server 1** – Address of the primary DNS server.
- **Received** – The number of data packets received on the WAN interface.
- **Transmitted** – The radio frequency of the WLAN transmission.

LAN – Display the basic LAN configuration settings.

- **MAC Address** – The physical layer address for the Mini AP Router's Ethernet port.
- **IP Address** – The IP address configured on the Mini AP Router.
- **Received** – The received LAN radio signal frequency.
- **Transmitted** – The radio frequency of the WLAN transmission.

WLAN – Display the wireless interface settings.

- **VAP1/VAP2** – The status of the Configuration.
- **ESSID** – The service set identifier for this wireless group.
- **Frequency** – The radio frequency of the WLAN transmission.
- **Transmit Power** – The power of the radio signals transmitted from the Mini AP Router. The higher the transmission power, the farther the transmission range.
- **Encryption Key** – The encryption used for broadcast and multicast data.

RAW Information — Click the button to display interface details and statistics.

Events Log

The Event Log page displays system messages generated during system operation. The logged messages can serve as a valuable tool for isolating Mini AP Router and network problems.

The screenshot displays the 'Events Log View' page for an Edge-Core WA2121 device. The top navigation bar includes tabs for System, Interfaces, Events log (which is active), DHCP Clients, PPPoE, WLAN Stations, and About. Below the navigation bar, the 'Events Log View' section shows a list of messages. The messages are timestamped and include details about system operations, such as DNS requests, DHCP offers, and system warnings. The messages are listed in chronological order, with the most recent at the top. The interface also includes a sidebar on the left with options for System, Status, and Reboot.

System	System	Interfaces	Events log	DHCP Clients	PPPoE	WLAN Stations	About
WAN	Events Log View						
LAN	Message Prefix:						
Wireless1	Jan 1 02:17:03	WA2121	daemon.info	dnsmasq[1629]:	DHCPREQUEST(br-lan) 192.168.1.138 00:13:f7:5f:5f		
Wireless2	Jan 1 02:17:03	WA2121	daemon.info	dnsmasq[1629]:	DHCPREQUEST(br-lan) 192.168.1.138 00:13:f7:5f:5f		
WMM	Jan 1 02:17:03	WA2121	daemon.info	dnsmasq[1629]:	DHCPREQUEST(br-lan) 192.168.1.138 00:13:f7:5f:5f		
QoS	Jan 1 02:17:03	WA2121	daemon.info	dnsmasq[1629]:	DHCPREQUEST(br-lan) 192.168.1.138 00:13:f7:5f:5f		
DMZ	Jan 1 00:01:46	WA2121	user.notice	miniupnpd[1779]:	listening on 192.168.1.1:5000		
Status	Jan 1 00:01:46	WA2121	user.info	Try 'iptables -h' or 'iptables --help' for more information.			
Reboot	Jan 1 00:01:46	WA2121	user.info	External IP =			
	Jan 1 00:01:46	WA2121	user.info	Bad argument 'eth0.2'			
	Jan 1 00:01:41	WA2121	daemon.warn	dnsmasq[1629]:	failed to access /tmp/resolv.conf.auto: No su		
	Jan 1 00:01:41	WA2121	daemon.info	dnsmasq[1629]:	using local addresses only for domain lan		
	Jan 1 00:01:41	WA2121	daemon.info	dnsmasq[1629]:	started, version 2.38 cachesize 150		
	Jan 1 00:01:41	WA2121	daemon.info	dnsmasq[1629]:	read /etc/hosts - 1 addresses		
	Jan 1 00:01:41	WA2121	daemon.info	dnsmasq[1629]:	compile time options: IPv6 GNU-getopt ISC-lea		
	Jan 1 00:01:41	WA2121	daemon.info	dnsmasq[1629]:	DHCP, IP range 192.168.1.100 -- 192.168.1.149		
	Jan 1 00:01:29	WA2121	user.warn	kernel:	ax531x_wdt: Watchdog timer is now enabled.		
	Jan 1 00:01:26	WA2121	authpriv.info	dropbear[1419]:	Running in background		
	Jan 1 00:01:25	WA2121	cron.notice	crond[1413]:	crond 2.3.2 dillon, started, log level 8		
	Jan 1 00:01:21	WA2121	syslog.info	syslogd	started: BusyBox v1.4.1		

Figure 5-25. Events Log View

The Events Log page displays the latest messages logged in chronological order, from the newest to the oldest. Log messages saved in the Mini AP Router's memory are erased when the device is rebooted.

DHCP Clients

The network information page displays the current Dynamic Host Configuration Protocol (DHCP) clients status. The displayed settings are for status information only and are not configurable on this page.

Edge-Core WA2121
Uptime: 2:47

Powered by Accion

System | **System** | Interfaces | Events log | **DHCP Clients** | PPPoE | WLAN Stations | About

DHCP Leases

MAC Address	IP Address	Name	Expires in
00:13:f7:5f:e5:b0	192.168.1.138	*	29min 42sec

DHCP Leases: DHCP leases are assigned to network clients that request an IP address from the DHCP server of the router. Clients that requested their IP lease before this router was last rebooted may not be listed until they request renewal of their lease.

Status

Reboot

Figure 5-26. DHCP Client Settings

PPPoE

The PPPoE Status page displays the current Point-to-Point Protocol over Ethernet (PPPoE) status. The displayed settings are for status information only and are not configurable on this page.

Edge-Core WA2121
Uptime: 2:48

Powered by Accion

System | **System** | Interfaces | Events log | DHCP Clients | **PPPoE** | WLAN Stations | About

PPPoE Status

PPPoE disabled.

Status

Figure 5-27. PPPoE Settings

WLAN Stations

The WLAN Stations page displays the wireless station status. The displayed settings are for status information only and are not configurable on this page.

Edge-Core

Powered by Action

Edge-Core WA2121
Uptime: 2:49

System

System

Interfaces

Events log

DHCP Clients

PPPoE

WLAN Stations

About

WAN

LAN

Wireless1

Wireless2

WMM

QoS

DMZ

Status

Reboot

WLAN Stations

Wireless1 stations

No.	MAC Addr	Channel	Rate	RSSI	Auth	Cipher	TXSEQ	RXSEQ	Associate Time
-----	----------	---------	------	------	------	--------	-------	-------	----------------

Wireless2 stations

No.	MAC Addr	Channel	Rate	RSSI	Auth	Cipher	TXSEQ	RXSEQ	Associate Time
-----	----------	---------	------	------	------	--------	-------	-------	----------------

Figure 5-28. Wireless Stations

About

The About page displays the software version and status installed in the Mini AP Router.

Edge-Core

Powered by Action

Edge-Core WA2121

Uptime: 2:51

System

System

Interfaces

Events log

DHCP Clients

PPPoE

WLAN Stations

About

WAN

LAN

Wireless1

Wireless2

WMM

QoS

DMZ

>>

Status

Reboot

About

Edge-Core WA2121

v1.0 - r642

This program is free software base on code from X-Wrt & OpenWrt; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

Figure 5-29. About

Reboot

The Reboot page allows you to restart the Mini AP Router software and restore factory default settings.

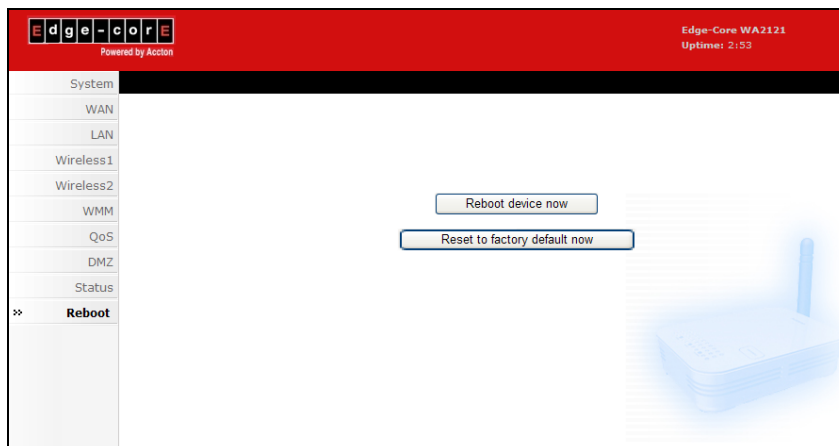


Figure 5-30. Reboot

The displayed items on this page can be described as follows:

- **Reboot Mini AP Router** – Click the Reboot button to reboot the system.
- **Restore Factory Settings** – Click the Factory Reset button to reset the configuration settings for the Mini AP Router to the factory defaults and reboot the system. Note that all user configured information will be lost. You will have to use the default IP address to re-gain management access to the Mini AP Router.

Note: If you have upgraded the system software, then you must reboot the Mini AP Router to implement the new code.

Appendix A: Troubleshooting

Check the following items before you contact local Technical Support.

1. If wireless clients cannot access the network, check the following:
 - Be sure the access point and the wireless clients are configured with the same Service Set ID (SSID).
 - If authentication or encryption are enabled, ensure that the wireless clients are properly configured with the appropriate authentication or encryption keys.
2. If the mini router cannot be configured using a web browser:
 - Be sure to have configured the access point with a valid IP address, subnet mask and default gateway.
 - If you are connecting to the mini router through the wired Ethernet interface, check the network cabling between the management station and the mini router. If you are connecting to mini router from a wireless client, ensure that you have a valid connection to the mini router.
3. If you forgot or lost the password:
 - Set the mini router to its default configuration by pressing the reset button on the bottom panel for 5 seconds or more. Connect to the web management interface using the default IP address 192.168.1.1. Then set up a new user name and password to access the management interface.
4. If all other recovery measure fail, and the mini router is still not functioning properly, take any of these steps:
 - Reset the mini router's hardware using the web interface or through a power reset.
 - Reset the mini router to its default configuration by pressing the reset button on the back panel for 5 seconds or more. Connect to the web management interface using the default IP address 192.168.1.1, then setup a user name and password.

Diagnosing LED Indicators

Troubleshooting Chart	
Symptom	Action
POWER LED is Off	<ul style="list-style-type: none">• The AC power adapter may be disconnected. Check connections between the Mini AP Router, the power adapter, and the wall outlet.
WLAN LED is Off	<ul style="list-style-type: none">• The Mini AP Router's radio has been disabled through it's web management interface. Access the management interface using a web browser to enable the radio.
LAN/WAN LED is Off (when port connected)	<ul style="list-style-type: none">• Verify that the Mini AP Router and attached device are powered on.• Be sure the cable is plugged into both the Mini AP Router and corresponding device.• Verify that the proper cable type is used and its length does not exceed specified limits.• Check the cable connections for possible defects. Replace the defective cable if necessary.

Appendix B: Specifications

Wireless Output Power

802.11b: 18 dBm (typical)

802.11g: 17 dBm @ 6 Mbps, 14dBm @ 54 Mbps

Wireless Receive Sensitivity

802.11b: -90 dBm @ 1 Mbps, -84 dBm @ 11 Mbps

802.11g: -86 dBm @ 6 Mbps, -68 dBm @ 54 Mbps

Operating Frequency

802.11g:

2.4 ~ 2.4835 GHz (US, Canada)

2.4 ~ 2.4835 GHz (ETSI, Japan)

802.11b:

2.4 ~ 2.4835 GHz (US, Canada)

2.4 ~ 2.4835 GHz (ETSI)

2.4 ~ 2.497 GHz (Japan)

Data Rate

802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per channel

802.11b: 1, 2, 5.5, 11 Mbps per channel

Operating Channels

802.11g:

11 channels in base mode (US, Canada)

13 channels (ETSI, Japan)

802.11b:

11 channels in base mode (US, Canada)

13 channels (ETSI)

14 channels (Japan)

Modulation Type

802.11g: CCK, BPSK, QPSK, OFDM

802.11b: CCK, BPSK, QPSK

AC Power Adapter

Input: 100-240 VAC, 50-60 Hz

Output: 5 VDC, 2 A

Unit Power Supply

DC Input: 5 VDC, 2 A maximum

Power Consumption: 6.5 W maximum

LED Indicators

POWER, LAN (Ethernet Link/Activity), WAN, (Ethernet Link/Activity), WLAN (Wireless Link/Activity)

Network Management

Web-browser

Temperature

Operating: 0 to 40 °C (32 to 104 °F)

Storage: -20 to 70 °C (32 to 158 °F)

Humidity

15% to 95% (non-condensing)

Compliances

FCC Part 15B Class B

EN 55022B

EN 55024

EN61000-3-2

EN61000-3-3

VCCI Class B

Radio Signal Certification

FCC Part 15C 15.247, 15.207 (2.4 GHz)

EN 300 328

EN 301 489-1

EN 301 489-17

ARIB STD-T66

IC RSS-210

Standards

IEEE 802.1 x

IEEE 802.11b, g

IEEE 802.3

Wi-Fi 11b/g, WPA, WPA2, WMM

Physical Size

12.5 x 7 x 2.7 cm (4.92 x 2.76 x 1.06 in)

Weight

170 g (6 oz)

Appendix C: License Information

This product includes copyrighted third-party software subject to the terms of the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other related free software licences. The GPL code used in this product is distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors. For details, refer to the section "The GNU General Public License" below, or refer to the applicable licence as included in the source-code archive.

The GNU General Public License

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

1. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

2. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

3. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a). You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- b). You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- c). If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

- 4. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
 - a). Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
 - b). Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,



- c). Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

5. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
6. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
7. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
8. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a

consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

9. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
10. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

11. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.



NO WARRANTY

1. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
2. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Glossary

10BASE-T

IEEE 802.3 specification for 10 Mbps Ethernet over two pairs of Category 3 or better UTP cable.

100BASE-TX

IEEE 802.3u specification for 100 Mbps Fast Ethernet over two pairs of Category 5 or better UTP cable.

Access Point

An internetworking device that seamlessly connects wired and wireless networks. Access points attached to a wired network, support the creation of multiple radio cells that enable roaming throughout a facility.

Advanced Encryption Standard (AES)

An encryption algorithm that implements symmetric key cryptography. AES provides very strong encryption using a completely different ciphering algorithm to TKIP and WEP.

Authentication

The process to verify the identity of a client requesting network access. IEEE 802.11 specifies two forms of authentication: open system and shared key.

Backbone

The core infrastructure of a network. The portion of the network that transports information from one central location to another central location where it is unloaded onto a local system.

Beacon

A signal periodically transmitted from the access point that is used to identify the service set, and to maintain contact with wireless clients.

Broadcast Key

Broadcast keys are sent to stations using dynamic keying. Dynamic broadcast key rotation is often used to allow the access point to generate a random group key and periodically update all key-management capable wireless clients.

Dynamic Host Configuration Protocol (DHCP)

Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

Encryption

Data passing between the access point and clients can use encryption to protect from interception and eavesdropping.

Ethernet

A popular local area data communications network, which accepts transmission from computers and terminals.

File Transfer Protocol (FTP)

A TCP/IP protocol used for file transfer.

Hypertext Transfer Protocol (HTTP)

HTTP is a standard used to transmit and receive all data over the World Wide Web.

IEEE 802.11b

A wireless standard that supports wireless communications in the 2.4 GHz band using Direct Sequence Spread Spectrum (DSSS). The standard provides for data rates of 1, 2, 5.5, and 11 Mbps.

IEEE 802.11g

A wireless standard that supports wireless communications in the 2.4 GHz band using Orthogonal Frequency Division Multiplexing (OFDM). The standard provides for data rates of 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps. IEEE 802.11g is also backward compatible with IEEE 802.11b.

Infrastructure

An integrated wireless and wired LAN is called an infrastructure configuration.

Local Area Network (LAN)

A group of interconnected computer and support devices.

MAC Address

The physical layer address used to uniquely identify network nodes.

Network Time Protocol (NTP)

NTP provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

Open System

A security option which broadcasts a beacon signal including the access point's configured SSID. Wireless clients can read the SSID from the beacon, and automatically reset their SSID to allow immediate connection to the nearest access point.

Orthogonal Frequency Division Multiplexing (OFDM)

OFDM allows multiple users to transmit in an allocated band by dividing the bandwidth into many narrow bandwidth carriers.

Repeater and Bridge

Repeater and bridge can provide an extended link to a remote access point from the wired LAN. Access Point working in this mode could connect to another AP in Access Point mode or Repeater and Bridge mode. Whenever there are two APs having wireless link together (one in Access Point or Repeater and Bridge mode, another using Repeater and Bridge mode), and also have wired link separately, these two APs are also working as “bridging” for the two wired links.

Service Set Identifier (SSID)

An identifier that is attached to packets sent over the wireless LAN and functions as a password for joining a particular radio cell; i.e., Basic Service Set (BSS).

Session Key

Session keys are unique to each client, and are used to authenticate a client connection, and correlate traffic passing between a specific client and the access point.

Shared Key

A shared key can be used to authenticate each client attached to a wireless network. Shared Key authentication must be used along with the 802.11 Wireless Equivalent Privacy algorithm.

Simple Network Time Protocol (SNTP)

SNTP allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

Temporal Key Integrity Protocol (TKIP)

A data encryption method designed as a replacement for WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.

Trivial File Transfer Protocol (TFTP)

A TCP/IP protocol commonly used for software downloads.

Virtual Access Point (VAP)

Virtual AP technology multiplies the number of Access Points present within the RF footprint of a single physical access device. With Virtual AP technology, WLAN users within the device's footprint can associate with what appears to be different access points and their associated network services. All the services are delivered using a

single radio channel, enabling Virtual AP technology to optimize the use of limited WLAN radio spectrum.

Wi-Fi Protected Access

WPA employs 802.1X as its basic framework for user authentication and dynamic key management to provide an enhanced security solution for 802.11 wireless networks.

Wired Equivalent Privacy (WEP)

WEP is based on the use of security keys and the popular RC4 encryption algorithm. Wireless devices without a valid WEP key will be excluded from network traffic.

WPA Pre-shared Key (WPA-PSK)

WPA-PSK can be used for small office networks with a limited number of users that may not need a high level of security. WPA-PSK provides a simple security implementation that uses just a pre-shared password for network access.

WA2121
E062007-EK-R01
149100040200E